NATIONAL WEATHER SERVICE POLICY DIRECTIVE 60-7

April 21, 2016

Information Technology

Information Technology Security Policy

NOTICE: This publication is available at: http://www.nws.noaa.gov/directives/.

OPR: OCIO (S. Richardson) **Certified by:** AOCIO (R.Varn)
Type of Issuance: Routine

SUMMARY OF REVISIONS: Supersedes NWS Policy Directive 60-7, Information Technology Security Policy, and dated December 12, 2011.

Changes made to reflect the NWS Headquarters reorganization effective April 1, 2015

1.0 This directive establishes the policy framework for the implementation, maintenance, and oversight of the National Weather Service (NWS) Information Technology (IT) Security Program.

2.0 NWS IT security policy derives from, and will henceforth be managed in accordance with, Department of Commerce (DOC) and National Oceanic & Atmospheric Administration (NOAA) IT security policies, standards, and practices, including DOC Commerce Interim Technical Requirements (CITRs). The DOC and NOAA IT security requirements are based upon Federal statute, including the Clinger-Cohen Act of 1996 and Federal Information Security Management Act (FISMA) of 2002; Federal regulatory requirements, including Office of Management and Budget (OMB) regulations and Federal Information Processing Standards (FIPS); and Special Publications of the National Institutes of Standards and Technology (NIST). These documents can be accessed at https://www.csp.noaa.gov/policies/ .

3.0 The Assistant Administrator for National Weather Services (AA/NWS) is responsible for ensuring the implementation of information security protection measures commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of NWS systems and information.

3.1 The Assistant Chief Information Officer (CIO) for Weather and NWS Portfolio Directors have been delegated as the Authorizing Officials (AOs) for moderate and low NWS IT systems under their direct control. For all high NWS IT systems, the NOAA CIO will serve as the Co-Authorizing Official (Co-AO). This authority cannot be further delegated.

3.2 The Assistant CIO for Weather has designated in writing a Chief Information Security Officer (CISO), Information Technology Security Officer (ITSOs) who will provide assistance to Portfolio Directors and staff in ensuring the development, implementation, maintenance, and reporting requirements established by Federal law, and DOC and NOAA IT Security policies, standards, and practices.

3.3 Portfolio Directors will appoint in writing qualified individuals to serve as System Owners and Information System Security Officers (ISSO) for all the information systems assigned to them. The ISSO will not function as the system administrator for any system which he/she serves as an ISSO to ensure separation of duties.

3.4 The System Owner will ensure the NWS system is documented and protected in accordance with Federal laws, and DOC, NOAA, and NWS policy.

3.5 System administrators will be assigned to systems for which they have been trained and have demonstrated competence to provide general IT support for operations. In addition, they are to provide technical assistance and implementation in the secure configuration of the systems and in response to security incidents as directed by authorized incident responders. A system administrator will not serve as ISSO on the same system.

4.0 Each user of NWS IT resources is responsible for understanding and complying with Federal IT security statutes and DOC and, NOAA, and NWS IT Security policies, standards, and practices. Any questions regarding compliance with these requirements documents should be raised with the user's immediate supervisor and then the system ISSO. If required, the ISSO will escalate the issue to the NWS ITSO and CISO.

5.0 This policy directive is supported by the references listed in Attachment 1.

_____signed_____ ____4/6/16_____
Louis W. Uccellini Date
Assistant Administrator for National Weather Services

Attachment 1

REFERENCES

The NWS Information Technology Security Policy is based upon Federal statutes, OMB regulations, and Federal Information Processing Standards as incorporated in the Department of Commerce and NOAA IT security polices, standards, and practices as set forth below. This list is not all inclusive.

- The Paperwork Reduction Act, 44 USC § 3501, et. seq.
- Federal Information Security Management Act of 2002
- Clinger Cohen Act of 1996
- The Privacy Act of 1974 as amended
- Office of Management and Budget Circular A-130, Appendix III, Management of Federal Information Resources
- U.S. Department of Commerce IT Security Program Policy and Minimum Implementation Standards
- U.S. Department of Commerce Information Technology Requirements (CITRS)
- U.S. Department of Commerce Physical Security Manual
- U.S. Department of Commerce Information Technology Security Manual
- U.S. Department of Commerce Information Technology Management Handbook
- Department Administrative Order 207-1, Security Programs
- NOAA Administrative Order 212-13, Information Technology Security Policy
- NOAA Information Technology Security Manual
- NWS Information Technology Directives
- Special Publications of the National Institute of Standards and Technology (NIST) as set out at http://csrc.nist.gov/publications/PubsSPs.html